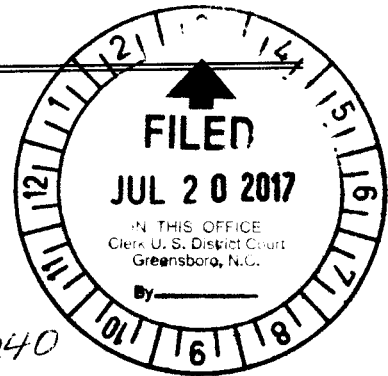


UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Email account: Timothy.Dowd7@gmail.com that is
stored on computer servers operated and controlled by
Google Inc.

Case No. 1:17 MJ 240

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Email account: Timothy.Dowd7@gmail.com that is stored on computer servers operated and controlled by Google Inc., located at 1600 Amphitheater Parkway, Mountain View, CA

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

The contents of electronic emails, other electronic data, and information more specifically described in Attachment B of this application.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|------------------------------|---|
| Title 18 USC, Section 875(c) | Transmitting/Communicating a Threat in Interstate or Foreign Commerce |

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SA Phillip W. Spainhour
Applicant's signature

Phillip W. Spainhour, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

7/20/2017

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake
Judge's signature

Joi Elizabeth Peake, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Phillip W. Spainhour, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since April 2008. Prior to the FBI, I was employed as a Detective/Deputy Sheriff by the Forsyth County Sheriff's Office in Winston-Salem, North Carolina, for over ten years. I attended and graduated from Gardner-Webb University with a Bachelor of Science in Sociology/Criminal Justice. I have completed hundreds of hours of training in numerous areas of law enforcement investigation and techniques, including but not limited to the following: Basic Law Enforcement Training through the State of North Carolina; Specialized training through the North Carolina Justice Academy; FBI New Agents Training in Quantico, Virginia; and Specialized Federal Law Enforcement training involving White Collar Crime, Public Corruption, Health Care Fraud, Evidence Response Team (ERT), Organized Crime Drug Enforcement Task Force (OCDETF), Money Laundering, Asset Forfeiture, Counterintelligence, Domestic and International Terrorism. I have participated in and conducted investigations of illegal activity involving drug trafficking, gang activity, and money laundering, public corruption, and

threats against the United States. Those investigations have led to indictment, arrest(s) and convictions of person(s) for various other criminal violations. Your affiant is currently assigned to the FBI Charlotte Division, Greensboro Resident Agency (GRA), Piedmont Triad Safe Streets Task Force (PTSSTF).

2. The facts in this affidavit come from my personal observations, my training and experience, and from information obtained from other agents, law enforcement agencies and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have participated in investigations related to threats made against Members of Congress to include violations of Title 18, U.S.C. § Section 875(c), which provides:

Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal investigation involving **Timothy George DOWD (hereinafter, DOWD)** for threatening Members of Congress, in violation of Title 18, U.S.C. § 875(c).

4. The facts and information contained in this affidavit are based upon my training and experience, participation in threats investigations,

personal knowledge, and observations during the course of this investigation, as well as the observations of other agents involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by my review of records, documents, and other physical evidence obtained during the course of this investigation. This affidavit contains information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the Government.

SOURCES OF INFORMATION

5. The statements in this affidavit are based on information provided to me by other Federal Bureau of Investigation Agents and United States Capitol Police ("USCP") Agents, local law enforcement officers, as well as my own investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On Friday, June 23, 2017 at approximately 2:27pm, DOWD sent an email to the United States Capitol Police (USCP) Public Information Office (PIO) in Washington, DC. The email was sent from the email address, Timothy.Dowd7@gmail.com with the subject line: "Target and assassinate Congress swine."

8. The email contained the following threatening statement:

"Plenty of us who hate the government filth that is ruining this country. I myself am coordinating and planning assassinations against the sub-human members of Congress. I just hate them and want them to die." Timothy Dowd

9. The USCP is the law enforcement agency in the legislative branch responsible for the protection of Members of Congress and the investigation of crimes against Members of Congress to include threats.

10. Witness 1, an employee in the USCP PIO office, reviewed the message and contacted the USCP Investigation Division- Threat Assessment Section (TAS) to report the threat for investigation.

11. Business subscriber records, provided by Google Inc., revealed the Internet Protocol (IP) address, 2606:a000:898f:9800:d150:4d64:7491:def2, as being accessed by the email address, Timothy.Dowd7@gmail.com to send the email. Google Inc. also provided the subscribers name as Timothy DOWD and

the phone number, 704-456-XXXX which was connected to DOWD through an open source search and law enforcement databases.

12. An open source search of the IP address revealed that the internet service provider for the address was located in Winston-Salem, North Carolina.

13. The internet service provider supplied the subscriber account information for the IP address 2606:a000:898f:9800:d150:4d64:7491:def2, which was accessed on June 23, 2017 at 2:27 p.m. The internet service provider identified the subscriber as William F. Dowd, Jr. with a billing address of 2037 Pembroke Forest Dr. Winston-Salem, NC and a phone number, 704-763-XXXX.

14. An open source search of the subscriber address, using the website Accurant, identified William and Geraldine Dowd as the owners of the residence. Timothy George DOWD was listed as a resident of this address.

15. A check of law enforcement databases, revealed DOWD had a history of making threats against the U.S. Government and U.S. officials. In 2007, DOWD was investigated by the United States Secret Service (USSS) for making threats against President George W. Bush, and the FBI. DOWD was interviewed by the USSS, and admitted posting the threatening statements on the internet, but denied any intent to carry out the threats. In 2010, DOWD was interviewed by the Bureau of Alcohol Tobacco Firearms and Explosives (BATFE), and FBI, for making statements on the internet about killing United

States Marines because of his opposition to the Iraq War. During the interview DOWD admitted making the statements, said he never should have made them, and that he had no intention of carrying out the threats. DOWD was not prosecuted for either the 2007 or 2010 incident.

16. On June 28, 2017, I conducted a spot-check surveillance of 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106. At approximately 7:48am, I observed a 2010 Chevrolet Corvette, bearing North Carolina License Plate: CAR-8142, Gray in color, leaving the area of the residence on Pembroke Forest Drive. The Corvette appeared to be driven by Timothy George DOWD. I followed the Corvette for several minutes and took a photograph of the vehicle at the intersection of University Parkway and Home Road, in Winston-Salem, NC.

17. Based on the facts above, there is probable cause to believe that DOWD violated 18 U.S.C. § 875(c), by communicating, in interstate commerce via his Gmail account, threats to assassinate members of Congress. There is further probable cause to believe that evidence related to the offenses described above is likely in the possession of GOOGLE.

18. As part of this investigation, USCP Special Agent Lawrence Anyaso obtained records linking DOWD to the email address Timothy.Dowd7@gmail.com.

19. Consistent with the forgoing, on June 28, 2017, Special Agent Anyaso requested, pursuant to 18 U.S.C. 2703(f), that GOOGLE. preserve records associated with the email account, Timothy.Dowd7@gmail.com.

20. On June 30, 2017 Special Agents with the FBI and USCP located DOWD at his residence 2037 Pembroke Forest Dr. Winston-Salem, NC, during the execution of a Federal search warrant. DOWD voluntarily consented to a non-custodial interview by the investigating Agents. During the interview, DOWD admitted one of the personal email addresses that he primarily used was Timothy.Dowd7@gmail.com. DOWD was asked if he was the only user of the personal email address he provided to interviewing agents, with included Timothy.Dowd7@gmail.com and he replied: "I should be the only one who uses them." DOWD admitted visiting websites and chat rooms focused on United States foreign policy issues. Those websites included, but were not limited to the following: Antiwar.com; Lewrockwell.com; and thesmirkingchimp.com. DOWD believed he used his email address to log into many of the websites he visited. DOWD admitted making comments and posts on websites that focused on U.S. foreign policy issues.

BACKGROUND CONCERNING EMAIL

21. In my training and experience, I have learned that GOOGLE provides a variety of on-line services, including electronic mail ("email") access, to the public. GOOGLE allows subscribers to obtain email accounts at the

domain name (gmail.com) like the email account listed in Attachment A. Subscribers obtain an account by registering with GOOGLE. During the registration process, GOOGLE asks subscribers to provide basic personal information. Therefore, the computers of GOOGLE are likely to contain stored electronic communications (including retrieved and unretrieved email for GOOGLE subscribers) and information concerning subscribers and their use of GOOGLE services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. I have learned that email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert

false information to conceal their identity this information often provides clues to their identity, location or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. I have learned that in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider

or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

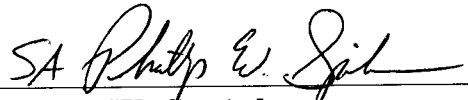
25. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and

timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on GOOGLE who will then compile the requested records at a time convenient to itself, reasonable cause exists to permit the execution of the requested warrant at any time of the day or night.

Respectfully submitted,



Phillip W. Spainhour

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me on this 20 day of July, 2017



The Honorable Joi Elizabeth Peake

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with TIMOTHY.DOWD7@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by GOOGLE Inc., a company located at 1600 Amphitheater Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by GOOGLE (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 28, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account on or after June 23, 2017, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of

connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored on or after June 23, 2017, by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 875 involving TIMOTHY GEORGE DOWD and occurring on or after June 23, 2017, as follow: for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications containing threats to U.S. Government officials, to include Members of Congress, or communications relating to or about such threats and any evidence of attempts to delete such communication;

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological

context of account access, use, and events relating to the crime under investigation and to the email account owner;

- (c) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY OF
DOMESTIC BUSINESS RECORDS PURSUANT TO
FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by GOOGLE, and my official title is _____. I am a custodian of records for GOOGLE. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of GOOGLE, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of GOOGLE; and

c. such records were made by GOOGLE as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature